EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIRST SECTION

CASE OF KULÁK v. SLOVAKIA

(Application no. 57748/21)

JUDGMENT

Art 8 • Private life • Home • Search of applicant's law firm and seizure of his work computer for a period of almost fifteen months, on the basis of the prosecutor's telephone consent, without a written search warrant • No immediate *ex post factum* judicial review of the lawfulness of, and justification for, searches of non-residential premises available at the relevant time • Seizure of entire work computer despite purpose of search being to secure computer data in relation to a criminal investigation • No domestic procedure ensuring the preservation of material unrelated to criminal proceedings and subject to legal professional privilege • Insufficient guarantees for applicant's Art 8 rights before or after the search-and-seizure operation despite a general basis for the impugned measure in domestic law • Interference not "in accordance with the law"

Prepared by the Registry. Does not bind the Court.

STRASBOURG

3 April 2025

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

In the case of Kulák v. Slovakia,

The European Court of Human Rights (First Section), sitting as a Chamber composed of:

Ivana Jelić, *President*,
Erik Wennerström,
Alena Poláčková,
Georgios A. Serghides,
Raffaele Sabato,
Frédéric Krenc,
Anna Adamska-Gallant, *judges*,
and Ilse Freiwirth, *Section Registrar,*

Having regard to:

the application (no. 57748/21) against the Slovak Republic lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Slovak national, Mr Tomáš Kulák ("the applicant"), on 23 November 2021;

the decision to give notice to the Slovak Government ("the Government") of the complaints under Article 8 of the Convention and to declare inadmissible the remainder of the application;

the parties' observations;

Having deliberated in private on 11 March 2025,

Delivers the following judgment, which was adopted on that date:

INTRODUCTION

1. The application concerns a search of the applicant's law firm and the seizure of his computer, carried out on the basis of the prosecutor's telephone consent, without a written search warrant. The computer, likely containing data subject to lawyer-client privilege, was returned to him fifteen months after its seizure. The applicant relied on Article 8 of the Convention.

THE FACTS

2. The applicant was born in 1980 and lives in Bratislava. He was represented by Ms Z. Mlkvá Illýová, a lawyer practising in Bratislava.

3. The Government were represented by their Agent, Ms Miroslava Bálintová, from the Ministry of Justice.

4. The facts of the case may be summarised as follows.

I. THE BACKGROUND TO THE CASE

5. On 20 August 2019 the National Crime Agency (*Národná kriminálna agentúra* – "NAKA") commenced an inquiry following suspicions that a number of individuals within and outside the judiciary had been accepting

bribes, abusing their official authority and interfering with the independence of the judiciary.

6. Further context to these events may be seen in the Court's decision in *Molnár v. Slovakia* ([Committee], no. 39818/20, 16 December 2020) and judgment in *Cviková v. Slovakia* (no. 615/21 and 2 others, 16 June 2024).

7. On 23 August 2019 a NAKA investigator appointed an electronics expert to draw up an expert report on the computers, mobile phones and other electronic devices secured for the purposes of the criminal case.

8. On 9 March 2020 a prosecutor of the Office of Special Prosecutions of the Prosecutor General's Office (*Úrad špeciálnej prokuratúry Generálnej prokuratúry*) charged eighteen people, including thirteen judges, with thirty counts of various offences linked to suspicions of corruption, abuse of official authority and interference with the independence of the judiciary. One of the cases for which charges were brought was the *Vodári* case, in which, according to the facts of the case, attempts were made by both parties to influence both sides of the proceedings. On 24 June 2020 former Judge S. testified as a cooperating witness and described the circumstances of the *Vodári* case, which he had dealt with as a first-instance judge and decided in favour of a defendant. According to Judge S., the applicant, as the legal representative of the defendant, had drafted a first-instance judgment, the defendant's interests having been supported by one of the accused judges.

II. SEARCH OF THE APPLICANT'S LAW FIRM

9. On 21 October 2020 the prosecutor of the Office of Special Prosecutions issued a warrant for the securing and surrendering of computer data (*príkaz na uchovanie a vydanie počítačových údajov*) pursuant to Article 90 § 1 (b) and (e) of the Code of Criminal Procedure, referring to all telecommunications devices, information technology devices and other data carriers used by the applicant. The warrant concerned all computer data, applications, text documents and audiovisual recordings stored in the memory of those devices which contained, even separately, keywords linked to the *Vodári* case. The purpose of the seizure was to gather data related to the commission of criminal acts connected to the *Vodári* case. The prosecutor justified the need for a warrant as follows:

> "It is necessary to secure the computer data on the applicant's electronic and telecommunications devices, as it is very likely that [he] could have written the [judgment] in question on his computers. Only this method is relevant for further evidence [to be collected] for the *Vodári* case ... The [Office of Special Prosecutions] does not intend to interfere with the applicant's work by taking away the aforementioned electronic devices, which would certainly make his work more difficult. For this reason, it is appropriate to proceed precisely by ordering the release of computer data from devices that the applicant is actively using. Devices that are no longer actively used, even if they are still in his possession, can be secured in kind. Gathering this data from the law firm's computers does not jeopardise legal professional privilege, since criminal proceedings can also protect this issue through the obligation

of police officers and experts to maintain secrecy. Moreover, not all data are downloaded from the electronic devices in question, only precisely specified data according to specific keywords. The collection of computer data is carried out by an expert in the relevant field.”

10. On 27 October 2020 the prosecutor charged ten people, including the applicant, with nineteen counts of various offences, including corruption, abuse of official authority and interference with the independence of the judiciary. The applicant was charged with the latter offence under Article 342 of the Criminal Code.

11. On the morning of 28 October 2020 law-enforcement officers searched the applicant’s law firm at his secondary address on Družstevná Street.

12. The parties differed in their descriptions of the events preceding the search.

13. According to the Government, law-enforcement officers went to the applicant’s home address, which was listed as the registered office of his law firm with the Slovak Bar Association. They had all the necessary legal means to secure the computer data at the registered office. Upon entering the applicant’s home and arresting him, the law-enforcement officers learnt from him that the actual location of his law firm and the work computer containing the data to be secured were at his secondary address on Družstevná Street. To prevent the destruction of evidence or the concealment of electronic devices, the law-enforcement officers had to move without delay to the secondary address. Subsequently, at this address, they learned from the applicant which office in the building was being used for his law firm. They therefore had no legitimate way to reliably verify whether anyone else was in the office or whether the computer data could be deleted remotely. For this reason, they had to act without delay and enter the law firm and search it.

14. The applicant submitted in his application form that the law-enforcement officers had arrived directly at his law firm on Družstevná Street, where they had arrested him while he was with a client in a meeting room in the building.

15. The search report indicated that the search had been conducted without a warrant, under Article 101 § 3 of the Code of Criminal Procedure, without, however, giving any further details regarding a legitimate urgency necessitating recourse to that procedure.

16. The search report described the search operation, which was conducted by five law-enforcement officers, including a forensic technician, in the presence of an independent observer and the electronics expert. At 9.25 a.m. a representative of the Slovak Bar Association was informed that a search would be carried out in the applicant’s law firm on Družstevná Street.

17. At 9.30 a.m. the applicant chose his legal representative, who confirmed at 9.35 a.m. that she would attend the search at his law firm. The law firm was closed at that time, and the applicant had the keys with him.

18. Subsequently, the applicant received the warrant dated 21 October 2021 (see paragraph 9 above) ordering the securing and surrendering of computer data from all telecommunications devices, information technology devices and other data carriers used by him.

19. At 10.10 a.m. the applicant's legal representative arrived at the law firm. She stated as follows:

> "... in the absence of a search warrant, we see no reason for voluntary cooperation in this matter, and once the warrant is presented, we have no problem cooperating."

20. At 10.10 a.m. the search began in the presence of the applicant, his legal representative, five police officers, an electronics expert and an independent observer.

21. At 10.20 a.m. a representative of the Slovak Bar Association arrived at the applicant's law firm.

22. At 10.25 a.m. the search was temporarily interrupted at the request of the applicant's legal representative so that she could speak with him in private.

23. The search was resumed at 10.45 a.m.

24. At 10.48 a.m. the representative of the Slovak Bar Association stated as follows:

> "I object to the lack of a written order to search other premises. On the basis of the above, it is not possible to establish the reason for the search and, in my opinion, the conditions for proceeding under Article 101 § 3 of the Code of Criminal Procedure are not fulfilled, as a result of which I can consider the procedure of the law-enforcement authorities to be unlawful. I would like to point out that any further action must take into account the lawyer's legal duty of confidentiality."

25. At 10.53 a.m. the applicant's legal representative said that she objected to the lack of precise specification of the computer from which the data were to be extracted.

26. Subsequently, the applicant and his legal representative requested that his work computer be secured without any interference.

27. At 11.10 a.m. the search was terminated.

28. During the search, the applicant's work computer was seized and fully secured. It contained data concerning various clients unrelated to the case under investigation.

29. The applicant countersigned the search report and was given a copy.

30. In a handwritten note dated 31 October 2020 the prosecutor stated that on the morning of 28 October 2020 the investigator had informed her by telephone of the search of the applicant's law firm under Article 101 § 3 of the Code of Criminal Procedure.

31. In a letter dated 6 November 2020 the investigator asked the expert to supplement his report in relation to the applicant's work computer, secured during the search on 28 October 2020, based on the keywords as having been specified in the warrant for the securing and surrendering of computer data.

32. On 18 November 2020, in reply to a complaint by the applicant dated 5 November 2020 challenging, under Article 210 of the Code of Criminal Procedure (review of police officers' actions by a prosecutor), the lawfulness of the search of his law firm and seizure of his work computer, the prosecutor stated that a search warrant for those premises could not have been obtained in advance as the actual place where he practised law had only been established after his arrest; according to the register of lawyers of the Slovak Bar Association, the registered office of his law firm was his place of residence. The prosecutor also stated that, owing to the size of the computer's hard drive, the expert present during the seizure of the computer data could not obtain the data directly on-site, meaning the entire computer had to be secured. The prosecutor further held that keywords had been specified to obtain the computer data, so any communication from the applicant unrelated to the criminal proceedings would be destroyed or returned to him upon request.

33. On 23 December 2020 the applicant lodged a constitutional complaint alleging, *inter alia*, violations of Articles 6 and 8 of the Convention by the procedure followed by NAKA and the Office of Special Prosecutions in connection with the search of his law firm and the seizure of his work computer.

34. On 5 March 2021 the applicant was notified of the decision by which the NAKA investigator had appointed the electronics expert to draw up an expert report (see paragraph 7 above) and of the letter of 6 November 2020 in which the investigator had asked the expert to supplement his report in relation to the applicant's work computer, secured during the search of 28 October 2020 (see paragraph 34 above).

35. On 25 March 2021, in reply to a request by the applicant dated 8 March 2021 for a review of the investigator's request to supplement the expert report under Article 210 of the Code of Criminal Procedure, the prosecutor from the Office of Special Prosecutions approved the procedural steps taken by the investigator, who had asked the appointed expert to supplement his report with information concerning the applicant's computer without issuing a new order for that procedural step.

36. On 20 May 2021 a prosecutor at the Prosecutor General's Office dismissed a complaint by the applicant dated 19 January 2021 challenging the lawfulness of the prosecutor's decision to charge him and the lawfulness of the warrant for the securing and surrendering of computer data, the search of his law firm and the securing of his work computer. The prosecutor clarified that the warrant for the securing and surrendering of computer data was not amenable to appeal. Moreover, he did not examine the lawfulness of the search of the applicant's law firm and seizure of his work computer, stating that this issue would be considered by the courts in the criminal proceedings against him.

37. On 25 May 2021 the Constitutional Court (I. ÚS 226/2021) dismissed the applicant's constitutional complaint, finding that he had had effective remedies at his disposal against NAKA's conduct, which he had used, and that there was therefore no reason for the court to intervene in the jurisdiction of the supervising prosecutor. As to the alleged violation of his rights by the conduct of the Office of Special Prosecutions, the court referred to its settled case-law, according to which criminal proceedings served, from start to finish, as a process through which law-enforcement authorities and courts could provide remedies by conducting individual measures and ensuring the protection of fundamental rights and freedoms, or even correct possible errors. Usually, it was only after criminal proceedings had been concluded that claims could be brought before the Constitutional Court regarding potential violations of fundamental rights and freedoms that had not been remedied in the course of the criminal proceedings.

38. The Constitutional Court replied to the applicant's arguments as follows:

> "... [the] Office of Special Prosecutions explained why it considered the investigator's procedure to have been lawful. It stated that the warrant under Article 101 § 1 could not have been obtained in advance because it had only been after the applicant's arrest that the actual place where he practised law had been established ...
>
> If the [police] in criminal proceedings have knowledge of a certain fact which they have no (apparent) reason to question ... they cannot be accused of passivity with regard to the verification of this fact ... Thus, if a situation arises in which the investigator learns of facts that were previously unknown to him – a different address for the applicant's law office – and it is necessary to secure the computer data on the computer at that address for the purposes of the criminal proceedings, this cannot be considered an approach that does not meet the requirements of Article 101 § 1 of the Code of Criminal Procedure.
>
> In this context, the Constitutional Court does not accept the applicant's argument that this was not an urgent measure. In the Constitutional Court's opinion, in such cases it is irrelevant when the act was committed or when the prosecution was initiated and how much time has passed since then ... because the decision to dispose of an item relevant to the criminal proceedings can only be taken in the case of a particular person at the time when the competent public authorities take certain steps that endanger the interests of that person in possession of the item.
>
> ...
>
> If the applicant sees a violation of ... his fundamental rights in the fact that [NAKA] retained his computer for an unreasonably long period, during which he had no access to it, and that this affected the performance of his work as a lawyer, the Constitutional Court notes that this situation was caused by the applicant and his defence counsel. In the [warrant] of 21 October 2020, the prosecutor's office justified the chosen method of securing the computer data by stating that it was not the intention of the prosecution authorities to cause damage to the performance of the work of the lawyer – the applicant – and to remove the electronic devices from him, which would certainly complicate his work. It was only in the course of the execution of ... the seizure of the computer equipment at the request of the applicant and his defence counsel, who insisted on the securing of the entire computer and its seizure (which the investigator complied with)

> – that a change took place, which later led to the situation with which the applicant expressed his dissatisfaction in the constitutional complaint, seeing in it an inadmissible interference with his fundamental rights ...
>
> The violation of the applicant's fundamental rights should have been caused by the seizure of the computer as a whole, which essentially resulted in the seizure of data unrelated to the criminal activity under investigation ... In the Constitutional Court's opinion, the correct specification of keywords for the successful selection and subsequent extraction of relevant computer data from the computer technology is a tool that sufficiently eliminates any undue interference with the constitutionally guaranteed right to the protection of privacy of third parties, although the occurrence of such interference cannot, of course, be absolutely excluded. In the present case, the prosecution authorities took the necessary measures to ensure the protection of the fundamental rights of the applicant, his clients and others and, in conjunction with the assurance of the destruction or return of irrelevant seized data, such a procedure must be regarded as constitutionally compliant.
>
> Moreover, the execution of the [warrant] of the [Office of Special Prosecutions] of 21 October 2020 was not carried out as such during the search of other premises, since the law-enforcement officers did not extract data from the computer, and the computer was fully secured ... to the satisfaction of the applicant, in order to prevent access to the data contained therein. In the absence of the execution of the [Office of Special Prosecutions'] warrant for the securing and surrendering of computer data, it cannot be regarded as an unacceptable interference with the applicant's fundamental rights.
>
> ...
>
> With regard to the applicant's remark that he had not been served with a search warrant ... and the report on the seizure ... the Constitutional Court notes that the search was carried out without a search warrant, as evidenced by the report on the execution of that procedural step. It is therefore obvious that the requested order could not have been served on him because of its absence."

39. The Constitutional Court concluded that no unacceptable violation of fundamental rights invoked by the applicant could occur as result of the conduct by or the warrant issued by the Office of Special Prosecutions.

40. On 2 August 2021 the expert submitted his expert report, which included an analysis of the applicant's work computer and elaborated on the keyword search. The content of the report showed that when examining the applicant's work computer, the expert went beyond the scope of the keywords specified in the warrant for the securing and surrendering of computer data, one of which was the applicant's surname, which resulted in the examination of computer data unrelated to the criminal proceedings against him. It appears that the applicant, his legal representative and/or a representative of the Slovak Bar Association were not involved in the keyword search, as domestic law did not provide for that possibility.

41. On 9 November 2021 the Constitutional Court (IV. ÚS 565/2021) rejected the applicant's second constitutional complaint, introduced on 9 June 2021, in which the applicant challenged the procedure followed by the Office of Special Prosecutions in appointing the expert in his case and in requesting him to supplement his report.

42. In a letter of 14 March 2022, the applicant informed the Court that his work computer had been returned to him on 21 January 2022. In his letter, the applicant also reiterated that the essence of his application was the interference by the public authorities consisting of the search of his law firm without a search warrant and the seizure of his work computer. The applicant further stated that the manner in which the expert had conducted his expert examination had interfered both with the applicant's right to privacy and with the professional privilege in relation to his clients.

43. On 30 March 2023 the applicant was officially indicted on charges of interference with judicial independence under Article 342 §§ 1 and 2 (b) of the Criminal Code. The criminal proceedings against him are still ongoing.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

THE CODE OF CRIMINAL PROCEDURE (AS IN FORCE AT THE RELEVANT TIME)

44. Article 90 § 1 defined the conditions for the securing and surrendering of computer data. It provided, *inter alia*, that if preserving stored computer data, including operational data stored through a computer system, was necessary for the clarification of facts necessary for the criminal proceedings, a warrant could be issued by a presiding judge or, prior to the initiation of the criminal prosecution or during the pre-trial stage, a prosecutor. The warrant had to be supported by the facts of the case and could be issued against a person in possession or having control over such data, or against a provider of such services. The warrant could order, *inter alia*, the creation and preservation of a copy of such data, and surrender of such data for the purposes of the criminal proceedings.

45. Article 93 provided that reports of measures taken under Articles 89 and 90 had to include a precise description of surrendered items, provided items or computer data to enable their identification. In addition, persons who had surrendered items or computer data, had had items or computer data seized from them or had handed over items or computer data had to be provided with written confirmation or a counterpart of the relevant report by the authority that had conducted the respective measure. Persons whose items or computer data had been secured had to be notified in writing by the authority that had taken control of the items or computer data.

46. Article 101 defined the conditions under which searches of non-residential premises and land could be carried out. Under Article 101 § 1, a search could be ordered by a warrant issued by a presiding judge or, prior to the initiation of the criminal prosecution or during the pre-trial stage, a prosecutor or a police officer with the prosecutor's consent. The warrant had to be issued in writing, state the reason for the search and be served on the owner or user of the premises, or on an employee thereof, at the time of

the search and, if this was not possible, within twenty-four hours after the obstacle to service had been resolved. Under Article 101 § 2, the search had to be conducted without delay by the authority that had ordered it or a police officer acting on its instructions.

47. Article 101 § 3 set out the situations in which searches could be carried out without prior authorisation. It stated that a police officer could conduct a search without a warrant or the consent referred to in Article 101 § 1 only when a warrant or consent could not be obtained in advance and the matter could not be delayed, or if it involved a person who had been caught in the act of committing a criminal offence or who was the subject of an arrest warrant or who was being pursued and was hiding in the premises in question. The police did, however, have to inform the authority empowered to issue the warrant or consent referred to in Article 101 § 1 without delay.

48. Article 105 defined the conditions for conducting searches and entering dwellings, non-residential premises and plots of land.

THE LAW

I. SCOPE OF THE CASE

49. In his reply to the Government's observations, which was lodged with the Court on 27 December 2023, the applicant referred to the Constitutional Court's decision of 9 November 2021 rejecting his second constitutional complaint concerning the procedure followed by the Office of Special Prosecutions in appointing the expert in the applicant's case and requesting him to supplement his report (see paragraph 41 above). He also noted that at the introduction of his application, the computer had still been in possession of the domestic authorities. Moreover, the Constitutional Court's decision had been delivered to him on 24 November 2021, the day following the introduction of the application. He finally noted that in their observations, the Government "[had] pre-empted the arguments concerning the violation of the substantive rights guaranteed by Article 8 of the Convention raised in essence in the second constitutional complaint". Accordingly, the case should be assessed also in the light of the arguments raised in the second constitutional complaint.

50. In reply, the Government maintained that the case could only be examined to the extent of the applicant's arguments raised in his first constitutional complaint. Relying on Rule 47 § 7 of the Rules of Court, they noted that in his submission of 14 March 2022, the applicant had not provided any information concerning his second constitutional complaint; the fact that the Constitutional Court's decision had been notified to him one day after the introduction of the application, and that his submission of 14 March 2022 had been submitted to the Court within a four-month time-limit after that notification, did not have any relevance. The Government made it clear that

they had commented on the applicant's statements in his letter of 14 March 2022 but not on "the violations alleged by [him] in the second constitutional complaint, as given by the impression of the applicant, since [they] were not ... aware of the filing of the second constitutional complaint ...".

51. The Court reiterates that allegations made after the expiry of the six-month[1] time-limit of the introduction of the application can only be examined by the Court if they constitute legal submissions relating to, or particular aspects of, the initial complaints that were introduced within the time-limit (see *Communauté genevoise d'action syndicale (CGAS) v. Switzerland* [GC], no. 21881/20, § 82, 27 November 2023).

The Court observers that the applicant introduced the present application on 23 November 2021 which is within the six months after the decision of the Constitutional Court of 25 May 2021 (see paragraph 37 above) on his first constitutional complaint in which he had complained of the procedure followed by NAKA and the Office of Special Prosecutions in connection with the search of his law firm and the seizure of his work computer (see paragraph 33 above).

52. The elements relating to the expert's appointment in the applicant's case in terms of an issue under Article 8 of the Convention were raised by the applicant for the first time in his observations on the admissibility and merits submitted to the Court on 27 December 2023 (see paragraph 49 above). They thus constitute a new complaint relating to the distinct matter under the provision relied upon and not an elaboration or elucidation of the applicant's original complaint, on which the parties have commented. The Court considers, therefore, that it cannot now take up this matter within the context of the present case (see *Radomilja and Others v. Croatia* [GC], nos. 37685/10 and 22768/12, §§ 122 and 129, 20 March 2018).

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

53. The applicant, relying on legal professional privilege, complained that the search of his law firm and the seizure of his work computer had violated his rights under Article 8 of the Convention, which reads as follows:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the

[1] Protocol No. 15 to the Convention, which entered into force on 1 August 2021, has amended Article 35 § 1 of the Convention to reduce the period for lodging an application from six to four months and, according to the transitional provisions of the Protocol (Article 8 § 3), this amendment applies only after a period of six months following the entry into force of the Protocol, that is starting from 1 February 2022.

> country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

A. Admissibility

54. The Court notes that the application is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. Parties’ submissions

(a) The applicant

55. The applicant argued that the domestic authorities’ conduct had not been in accordance with the law because no effective protection against arbitrary interference had been available under domestic law in connection with the search of his law firm, the seizure of computer data and the subsequent conduct of the investigating authorities.

56. He admitted that his presence and that of his legal representative and a representative of the Slovak Bar Association during the search could be taken into account as a factor enabling him to effectively control the extent of the search, but that this fact alone was not sufficient *per se* in the absence of prior court authorisation and a subsequent effective judicial review. He pointed out, in that connection, that he and the representative of the Slovak Bar Association had consistently argued that the search was contrary to domestic law, since the conditions for carrying it out without a warrant under Article 103 § 3 of the Code of Criminal Procedure had not been met. However, their arguments had been merely noted and the search had continued.

57. The applicant maintained that the criminal investigation had started on 20 August 2019, which raised significant doubts as to whether the investigator could not have applied for a warrant before the search. Moreover, no immediate *post factum* judicial review had been available under domestic law, since his complaint under Article 210 of the Code of Criminal Procedure had been addressed to the prosecutor, and the Constitutional Court had deferred him to further stages of the criminal proceedings, which, in his view, did not constitute effective procedural guarantees in his case.

58. The applicant further argued that domestic law and practice had not offered him effective protection as regards the seizure of computer data and subsequent conduct of the investigating authorities. However, he did not dispute the fact that a seizure of data could be carried out if there was a reasonable suspicion that something relevant to criminal proceedings would be found.

59. The applicant admitted that he had suggested that the work computer be taken in its entirety at the end of the search. He stressed, however, that he had done so in reliance on the prosecutor's statement that it would be returned to him within a short time.

60. The applicant further stated that domestic law did not provide for an obligation to separate data carriers used in the provision of legal services in order to facilitate the sifting process. Furthermore, there had been no possibility under domestic law for him or his representative to be present during the keyword search. Nor did domestic law provide any guidance on how the potential disputes between the investigative authorities and the lawyer concerned over the keywords to be used or any other methods of filtering the electronic content should be resolved. In addition, since no possible appeal to a judicial authority was available against investigative activities, it did not follow from domestic law that material in respect of which the applicability of legal professional privilege was disputed would not be made available to the investigating authorities before the domestic courts had had a chance to conduct a specific and detailed analysis of the matter, and – if necessary – order the return or destruction of seized data carriers and their copied content.

61. The applicant also pointed out that the Constitutional Court had referred to the prosecutor's statement that the unrelated data would be destroyed or returned, despite the fact that such destruction had no basis in domestic law and no data had been destroyed or returned until the conclusion of the expert examination. The applicant concluded that domestic law had lacked the procedural guarantees relating specifically to the protection of legal professional privilege and, therefore, had not been in accordance with the law as provided for in Article 8 § 2 of the Convention.

(b) The Government

62. The Government submitted that the search warrant could not have been obtained in advance because the applicant's actual place of practising law had only become known after his arrest. Prior to the applicant's arrest, the law-enforcement authorities had known that he had been staying at his permanent residence, which had also been the registered address of his law firm. According to the Government, the law-enforcement authorities had taken all the necessary legal prerequisites for securing the necessary computer data in the registered office of the applicant's law firm, but their precise specification could not be provided as they had been subject to national law requiring confidentiality. The law-enforcement authorities had had no reason to presume that the registered office of the law firm was not the same as its actual office. They had not monitored the applicant prior to his arrest and had therefore had no knowledge that he had not been practising law at the registered office.

63. Only after they had entered the applicant's home had the law-enforcement officers learnt from him that he had been practising law at his secondary address, where his computer had also been located. Therefore, in order to prevent the destruction of evidence or the concealment of the device in question, the law-enforcement officers had gone without delay to the applicant's law firm at the secondary address. The Government stated that there had been no other legitimate way for the law-enforcement officers to reliably check whether there was anyone else in the office or whether the computer data could be deleted remotely. The matter could not therefore be delayed, so the police had proceeded to enter and search the premises. The prosecutor had immediately been informed of the search of the law firm, as required by Article 101 § 3 of the Code of Criminal Procedure.

64. The Government further maintained that the warrant for the securing and surrendering of computer data had been issued pursuant to Article 90 § 1 (b) and (e) of the Code of Criminal Procedure. It had been issued in writing, had specified the devices and media from which the computer data were to be obtained, the specific data to be obtained, including the defined keywords to be included in the data, and had been reasoned.

65. They also submitted that the search of the applicant's law firm and the seizure of his computer had served a legitimate purpose, namely the prevention of crime. In the *Vodári* case, serious suspicions of manipulation of court proceedings and corruption in the judiciary had been raised. In view of the objective of the criminal activities under investigation, securing computer data by searching the law firm and seizing the applicant's computer had appeared to be the only means of achieving the intended objective. The purpose of the search of the law firm and the seizure of his computer had been to obtain the data stored on the computer in question. The search had been carried out in the law firm and no other evidence had been secured during the search.

66. Moreover, the Government argued that, as indicated in the warrant, the law-enforcement authorities had intended to secure only certain computer data described therein using keywords. The securing had not therefore been meant to encompass the entire contents of the applicant's computer, as had been made clear in the wording. However, owing to the large size of the hard drive, the expert had been unable to use the specified measure during the search of the law firm, necessitating the computer's seizure. In this regard, the Government noted that, during the search, both the applicant and his legal representative had insisted that the computer be taken and fully secured.

67. After the seizure of the applicant's computer, the investigator, in a request dated 6 November 2000, had asked the expert to supplement his expert examination, *inter alia*, by examining it. In his request, the investigator had repeated the keywords previously indicated in the search warrant. However, according to the investigator's statement, the expert had not only followed the incorrect procedure during the examination of the applicant's

computer, he had also incorrectly used keywords intended for the expert examination of other devices seized in the course of the relevant criminal proceedings. As a result of the expert's misconduct, data had been included in his report that had not been requested by the investigator. The investigator had only discovered this after receiving the report, that is, when it had already been prepared and, therefore, he could no longer objectively correct the expert's behaviour and could not arbitrarily change the expert's report.

68. In this context, the Government noted that when conducting expert examination, an expert did not act as a public authority, but as an independent entity that is merely authorised by the State to carry out activities in accordance with the Act on Experts, Interpreters and Translators. Pursuant to this Law, an expert must perform his expert activities in a proper manner and was liable for damages that might arise in connection with the performance of his expert activities under a liability insurance policy. Any dispute that might arise was of a private nature and could be resolved by a national court on the basis of an action for damages brought by the applicant.

69. Furthermore, the Government admitted that the applicant's computer had been kept for a longer period than the law-enforcement authorities had initially estimated. This delay had been caused by the fact that the appointed expert had carried out an examination of several secured devices belonging to different accused persons, which had objectively taken longer.

70. Lastly, the Government submitted that the applicant had had at his disposal an effective guarantee for the protection of his rights – a request for a review of the investigator's conduct under Article 210 of the Code of Criminal Procedure, which he had in fact used. The prosecutor had reviewed the challenged conduct of the investigator and explained why she considered that conduct to have been lawful.

71. The Government concluded that domestic legislation and practice had provided the applicant with an effective guarantee against arbitrary interference with his rights under Article 8 of the Convention.

2. *The Court's assessment*

(a) Preliminary remark

72. The Court notes at the outset that the parties differed in their description of the events preceding the search of the applicant's law firm (see paragraphs 13 and 14 above). The Court considers it appropriate to rely on the Government's version of events, which was not disputed by the applicant in his observations in reply to those of the Government.

(b) General principles

73. According to the Court's well-established case-law, searches and seizures carried out on the premises of a lawyer's office constitute an interference with the rights protected by Article 8 of the Convention

(see *Niemetz v. Germany*, 16 December 1992, §§ 29-33, Series A no. 251-B; *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 64, ECHR 2003-IV; *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, § 43, ECHR 2007; *André and Another v. France*, no. 18603/03, § 37, 24 July 2008; *Xavier Da Silveira v. France*, no. 43757/05, § 32, 21 January 2010; *Heino v. Finland*, no. 56720/09, § 33, 15 February 2011; *Golovan v. Ukraine*, no. 41716/06, § 51, 5 July 2012; *Močuļskis v. Latvia*, no. 71064/12, §§ 40-41, 17 December 2020; and *Särgava v. Estonia*, no. 698/19, § 85, 16 November 2021).

74. The Court notes that, in comparable cases, it has examined whether national legislation and practice afforded appropriate and sufficient safeguards against abuse and arbitrariness (see, *inter alia*, *Miailhe v. France (no. 1)*, 25 February 1993, § 37, Series A no. 256-C; *Funke v. France*, 25 February 1993, § 56, Series A no. 256-A; *Crémieux v. France*, 25 February 1993, § 39, Series A no. 256-B; *Ste Colas Est and Others v. France*, no. 37971/97, § 48, 16 April 2002; and *Wieser and Bicos Beteiligungen GmbH*, cited above, § 57). The Court has also held that these safeguards include the existence of an "effective review" of measures contrary to Article 8 of the Convention (see *Lambert v. France*, 24 August 1998, § 34, *Reports of Judgments and Decisions* 1998-V).

75. Moreover, the Court reiterates the importance of specific procedural safeguards when it comes to protecting the confidentiality of exchanges between lawyers and their clients, as well as professional secrecy (see, *inter alia*, *Särgava*, cited above, § 88; *Sommer v. Germany*, no. 73607/13, § 56, 27 April 2017; and *Michaud v. France*, no. 12323/11, § 130, ECHR 2012). It emphasises that, under Article 8 of the Convention, correspondence between a lawyer and his client and, more generally, all forms of communication between them, whatever their purpose, enjoy a privileged status as regards their confidentiality (see *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*, no. 277013/10, § 77, 3 September 2015; *Niemietz*, cited above, § 32; and *Campbell v. the United Kingdom*, 25 March 1992, §§ 46-48, Series A no. 233). Moreover, it attaches particular importance to the risk of breaches of legal professional privilege, since it is the basis of the relationship of trust between lawyer and client (see *Xavier Da Silveira*, § 36, and *André and Another*, § 41, both cited above) and may affect the proper administration of justice (see *Sérvulo & Associados - Sociedade de Advogados, RL and Others*, § 77; *André and Another*, § 41; *Wieser and Bicos Beteiligungen GmbH*, §§ 65-66; and *Niemietz*, § 37, all cited above).

76. In that connection, the Court has already held that the Convention does not prohibit the imposition on lawyers of certain obligations likely to concern their relationships with their clients. This is the case in particular where credible evidence is found of the participation of a lawyer in an offence, or in connection with efforts to combat certain practices. On that

account, however, it is vital to provide a strict framework for such measures, since lawyers occupy a vital position in the administration of justice and can, by virtue of their role as intermediary between litigants and the courts, be described as officers of the law (see *Särgava*, cited above, § 89, with a further reference). The Court has repeatedly held that since persecution and harassment of members of the legal profession strikes at the very heart of the Convention system, the searching of lawyers' premises should be subject to especially strict scrutiny (see *Heino*, cited above, § 43 with further references), which implies the presence and effective participation of an independent qualified observer (see *Golovan*, cited above, §§ 62-63 with further references). More specifically, such an observer must, in addition, have legal qualifications in order to be able to participate effectively in the proceedings and be empowered to prevent any interference with the professional secrecy of the lawyer whose chambers are searched (see ibid., § 63, with further references).

77. Lastly, the Court must take account of the extent of the possible repercussions on the work and reputation of the person searched (see *Camenzind v. Switzerland*, 16 December 1997, § 45, *Reports* 1997-VIII; *Buck v. Germany*, no. 41604/98, § 45, ECHR 2005-IV; *Smirnov v. Russia*, no. 71362/01, § 44, 7 June 2007; *Wieser and Bicos Beteiligungen GmbH*, cited above, § 57; *Iliya Stefanov v. Bulgaria*, no. 65755/01, § 38, 22 May 2008; *Aleksanyan v. Russia*, no. 46468/06, § 214, 22 December 2008; and *Kolesnichenko v. Russia*, no. 19856/04, § 31, 9 April 2009).

(c) Application of the general principles to the present case

(i) Existence of an interference

78. The Court notes at the outset that the Government did not dispute that the search of the applicant's law firm and the retention of his work computer for a period of almost fifteen months fall within the scope of Article 8 of the Convention, and that they constituted an interference by the State with the applicant's right to respect for his private life, home and correspondence. The Court sees no reason to hold otherwise.

79. Such interference violates this provision unless it is in accordance with the law, pursues one or more of the legitimate aims set out in Article 8 § 2, and is necessary in a democratic society in order to achieve the aim or aims concerned.

(ii) Existence of a legal basis and procedural safeguards in domestic law

80. The Court reiterates that, according to its well-established case-law, the expression "in accordance with the law" requires that the measure in question must have a basis in domestic law (and must not merely be a practice without a specific legal basis, see *Heglas v. the Czech Republic*, no. 5935/02, § 74, 1 March 2007). The measure must also be compatible with the rule of

law, which is expressly referred to in the Preamble to the Convention and is inherent in the object and purpose of Article 8 (see, in particular, *Bykov v. Russia* [GC], no. 4378/02, § 76, 10 March 2009; *Saber*, cited above, § 50; *Kruslin v. France*, 24 April 1990, §§ 30 and 32, Series A no. 176-A; and *Huvig v. France*, 24 April 1990, §§ 29 and 31, Series A no. 176-B). The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 228, ECHR 2015, and *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000-V).

81. Turning to the circumstances of the present case, the Court observes that the search of the applicant's law firm was carried out without a prior search warrant for non-residential premises, in accordance with the urgency exception under Article 101 § 3 of the Code of Criminal Procedure at the relevant time (see paragraph 47 above), to secure computer data from electronic devices belonging to or used by the applicant, on the basis of a warrant for that purpose issued by the prosecutor of the Office of Special Prosecutions on 21 October 2020 pursuant to Article 90 § 1 (b) and (e) of the Code of Criminal Procedure (see paragraphs 9 and 41 above). Therefore, the Court finds that the search-and-seizure interference had some formal basis in national law.

82. The Court has considered that in cases where domestic legislation does not provide for prior judicial scrutiny of the lawfulness and necessity of an investigative measure, other safeguards have to be in place (see *Modestou v. Greece*, no. 51693/13, § 48, 16 March 2017). It has also held that the absence of a prior warrant may be counterbalanced by the availability of an effective and diligently conducted *ex post factum* judicial review of the lawfulness of, and justification for, the search warrant (see *Heino*, cited above, § 45; *Gutsanovi v. Bulgaria*, no. 567270/09, § 222, 15 October 2013; *Modestou*, cited above, § 49; and *Bostan v. the Republic of Moldova*, no. 52507/09, § 25, 8 December 2020). It reiterates in this regard that, notwithstanding the margin of appreciation which it recognises the Contracting States have in this sphere, it must be particularly vigilant where, as in the present case, the authorities are empowered under national law to order and effect searches without a judicial warrant. If individuals are to be protected from arbitrary interference by the authorities with the rights guaranteed under Article 8, a legal framework and very strict limits on such powers are called for (see *Gutsanovi*, cited above, § 220, with further references).

83. The Court acknowledges that the search conducted in the present case was accompanied by certain formal procedural safeguards. It was carried out by five law-enforcement officers, including a forensic technician, in the presence of an independent observer, an electronics expert (see paragraph 16 above) and a representative of the Slovak Bar Association (see paragraphs 17 and 21 above). The applicant and his legal representative were also present

throughout the entire search. Furthermore, it appears from the documents in the Court's possession that the prosecutor was informed of the search by the law-enforcement officers by telephone (see paragraph 30 above). It remains unclear, however, how extensive their communication was and whether it had taken place before the search, during it or after it had been completed. In any event, it appears to have been a formal notification as required by Article 101 § 3 of the Code of Criminal Procedure in force at the relevant time. The applicant challenged the search of his law firm in his complaint to the prosecutor under Article 210 of the Code of Criminal Procedure, but, as has already been noted, the prosecutor's reply did not refer to any relevant circumstances justifying the urgent intervention in the applicant's law firm (see paragraph 32 above).

84. The Court observes that there was no immediate *ex post factum* judicial review of the lawfulness of, and justification for, searches of non-residential premises, such as law firms, available in Slovakia at the relevant time. Supervision of the lawfulness and effective protection against arbitrary interference with the applicant's rights under Article 8 of the Convention was provided by the prosecutor at the pre-trial stage and by the courts after the filing of the indictment. The Court considers, however, that under Slovak law the public prosecutor does not have an independent status comparable to that of an independent tribunal within the meaning of Article 6 of the Convention. Moreover, any opportunity for the applicant to challenge the warrant or any aspect of its implementation in the criminal proceedings against him would have concerned the protection of his right to a fair hearing in the determination of the criminal charge against him, which is not at issue in the present case, but would have had no direct bearing on his rights protected independently under Article 8 of the Convention (see *Plechlo v. Slovakia*, no. 18593/19, § 46, 26 October 2023). A system of *ex post factum* judicial approval is now provided for in Article 101 § 2 of the Code of Criminal Procedure, as amended by Law no. 40/2024, which entered into force on 15 March 2024[2].

85. The search of the applicant's law firm led to the seizure of his work computer, which, according to him, contained client files that were not relevant to the criminal proceedings against him. In this connection, the Court observes that the presence of the representative of the Slovak Bar Association during the search, who undoubtedly had the necessary legal qualifications to participate effectively in the proceedings and who was bound by lawyer-client privilege to ensure the protection of privileged material and the rights of third parties (see *Golovan*, cited above, § 63, with further references), was purely symbolic and formal since, under the provisions of the Code of Criminal Procedure in force at the relevant time, he was not

[2] Law no. 40/2024 also newly introduced, in Article 101 § 1 of the Code of Criminal Procedure, a prior judicial warrant in order to carry out a search in non-residential premises.

entitled to interfere in any way with the search of the law firm and seizure of the applicant's work computer to ensure the practical and effective protection of the confidential information contained therein likely to be covered by lawyer-client privilege[3].

86. The law-enforcement officers secured the applicant's entire work computer, despite the fact that the purpose of the search of his law firm was to secure computer data under the terms of the prosecutor's warrant for that purpose of 21 October 2020. In the Court's view, it is irrelevant that the applicant and his legal representative requested that the computer be secured without any interference, as the law-enforcement officers were well aware that the applicant was a lawyer, and it is for the State to ensure a strict framework for such searches to be carried out (see *André and Another*, cited above, § 42).

87. The expert then analysed the computer data on the basis of the keywords indicated in the prosecutor's warrant (see paragraph 9 above). Despite the Government's submission to the contrary, there is no information to warrant the conclusion that only relevant information was accessed on the applicant's computer. The Court observes, in this regard, that, at the relevant time, domestic law did not provide for any procedure to ensure that material unrelated to ongoing criminal proceedings and subject to legal professional privilege be preserved (compare and contrast *Wieser and Bicos Beteiligungen GmbH*, cited above, §§ 62-63, as regards safeguards laid down by law, and *Wolland v. Norway*, no. 39731/12, §§ 38 and 63, 17 May 2018).

88. The Court adds that the deficiencies in the Slovakian legal system with regard to the protection of computer data subject to legal professional privilege are evidenced in the present case by the error made by the expert appointed by the State to act in the context of criminal proceedings brought against the applicant. This error was reflected in the results of his examination, which, according to the Government, could not be corrected, resulting in the applicant having to bear the consequences. Lastly, the Court considers that the expert's workload, relied on by the Government, cannot plausibly explain why the applicant's work computer was returned to him after almost fifteen months, which inevitably had negative repercussions on his work as a lawyer (see, *mutatis mutandis*, *Q and R v. Slovenia*, no. 19938/20, § 79, 8 February 2022, with further references).

89. Bearing in mind the above, the Court is of the view that even though there existed a general basis in Slovakian law for the impugned measure, the applicant in the present case was not offered sufficient guarantees for his right to respect of his private life and home before or after the search-and-seizure operation. In these circumstances, the Court finds that the interference with his right to respect for his private life and home was not "in accordance with

[3] The effective involvement of a representative of the Slovak Bar Association in searches of law firms was newly included in the Code of Criminal Procedure in Article 106a by Law no. 111/2023 with effect from 1 May 2023.

the law", as required by Article 8 § 2 of the Convention. Having drawn that conclusion, it is not necessary for the Court to review compliance with the other requirements under that provision.

90. Accordingly, the Court finds that there has been a violation of Article 8 of the Convention.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

91. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

92. The applicant claimed 10,000 euros (EUR) in respect of non-pecuniary damage.

93. The Government considered this claim overstated and requested that the Court, should it find a violation of the Convention, award the applicant appropriate compensation.

94. The Court, ruling on an equitable basis, awards the applicant EUR 10,000 in respect of non-pecuniary damage, plus any tax that may be chargeable.

B. Costs and expenses

95. The applicant also claimed EUR 7,000 for costs and expenses incurred before the domestic courts and the Court.

96. The Government maintained that the applicant had not documented that he had actually paid that sum.

97. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 3,125 covering costs under all heads, plus any tax that may be chargeable to the applicant.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 8 of the Convention;

3. *Holds*

   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts at the rate applicable at the date of settlement:

      (i) EUR 10,000 (ten thousand euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;

      (ii) EUR 3,125 (three thousand one hundred and twenty-five euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;

   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

4. *Dismisses* the remainder of the applicants' claim for just satisfaction.

Done in English, and notified in writing on 3 April 2025, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Ilse Freiwirth Registrar	Ivana Jelić President